CLAIMS

1. A method of controlling access to a specific resource on a mobile telephone; comprising the steps of:

(a) associating an identity with a permission state, in which an identity is a label applicable to one of several entities on whose behalf the resource could potentially be used and the permission state defines whether or not the resource can actually be used; and

(b) allowing use of the resource solely to an entity or entities labelled with an identity associated with a permission state that does permit such use.

2. The method of Claim 1 comprising the steps of

(a) a script or other kind of executable code associated with a given entity sending a request to use the specific resource; the script being labelled with an identity or including a secure signature from which an identity can be deduced;

(b) a software component running on the device processing the request and using the identity to determine the applicable permission state associated with the identity for that script or executable code.

3. The method of any preceding Claim in which the permission state includes a permission type and a value.

4. The method of any preceding Claim in which a permission state associated with a given identity can be updated or altered.

5. The method of Claim 4 in which the updating or alteration of a permission state is done on instructions sent from a computer remote from the mobile telephone.

6. The method of any preceding Claim in which use of the resource includes one or more of: access, deployment, alteration or deletion.

7. The method of Claim 2 in which the script or other kind of executable code associated with a given entity is labelled with an additional identity separate from or independent of the identity of the given entity; the additional label identifying the script or code.

8. The method of Claim 7 in which the component can use the permission state associated with the additional identity to enable it to determine if the script itself is permitted to use the resource, irrespective of whether the given entity is allowed to use the resource.

9. The method of Claim 2 in which the script or code can have its identity altered.

10. The method of Claim 9 in which the alteration is a result of instructions sent to the telephone from a remote computer.

11. The method of Claims 9 or 10 in which the identity is altered to an identity associated with a higher or broader permission state only if the script or code has been authenticated to a pre-defined confidence level.

12. The method of Claim 2 in which the method is deployed on the mobile telephone by a component that is not part of the operating system and can therefore be installed onto the telephone without needing to be burnt into the main ROM of the telephone that stores the operating system.

13. The method of Claim 12 in which the component runs in the secure SIM of the mobile telephone.

14. The method of Claim 12 in which the permission states and their association with different identities are stored in the SIM, but the component runs outside the SIM.

15. The method of Claim 14 further comprising the step of remotely administering the permission states associated with different identities, by sending instructions from a computer remote from the computer.

16. The method of Claim 2 in which the component stores in memory, or accesses from memory a list of the permission states associated with different identities.

17. The method of Claim 2 in which an identity is determined for any script that seeks to access code by an authentication process using a digital signature.

18. The method of Claim 17 in which the authentication process generates an identity handle that can be transferred as a token.

19. The method of Claim 18 in which the identity handle has an associated confidence level based on the authentication.

20. The method of Claim 1 in which the entity is an individual end-user.

21. The method of Claim 1 in which the entity is a network operator.

22. The method of Claim 1 in which the entity is a mobile telephone manufacturer.

23. The method of Claim 1 in which the entity is an application developer or vendor.

23. The method of Claim 1 in which the entity is an employer.

24. The method of Claim 1 in which the entity is an operation

25. The method of Claim 24 in which the operation is booting the telephone so that startup code is run, the startup code having a specific identity, and the permissions for this identity determine what can or cannot be done at startup.

26. The method of Claim 1 in which the entity is an operation of a timer going off.

27. The method of any preceding Claim in which the entity is a kind or type of entity.

28. The method of any preceding Claim in which at least two entities do not have identities that are associated with permission states that are hierarchically arranged with respect to each other.

29. The method of any preceding Claim in which no entities have identities that are associated with permission states that are hierarchically arranged with respect to each other.

30. The method of any preceding Claim in which no entity automatically has rights to use all resources on the telephone.

31. The method of any preceding Claim in which the resource is specific data.

32. The method of Claim 31 in which the permission state determines whether the data can be read, modified or deleted.

33. The method of any preceding Claim 1 - 32 in which the resource is a specific executable application and the permission state determines whether the application can be run or updated.

34. The method of any preceding Claim in which the resource is a hardware resource on the telephone.

35. The method of any preceding Claim in which the resource is a networking or communications resource on the telephone.

36. The method of any preceding Claim in which the step of associating an identity with a permission state results in a record of the association stored in a memory of the telephone.

37. The method of any preceding Claim in which the step of allowing use of the resource takes place by a CPU in the telephone processing data.

38. A mobile telephone with specific resources, in which access to the resources is controlled using the method of any preceding Claim 1 – 37.